Exhibit 16

Electronic Frontier Foundation

November 30, 2005

Jeffrey P. Cunard, Esq.
Debevoise & Plimpton LLP
555 13th Street, N.W.
Suitc 1100 East
Washington, D.C. 20004

RE: MediaMax Security Vulnerability

Dear Jeff:

Previously, you asked EFF to inform you as soon as possible if we had discovered any security risks due to SunComm's technology.

We are writing to inform you that installation of the SunnComm MediaMax software, version 5, creates a serious risk of a "privilege escalation attack." The problem may also exist for other versions of the software as well.

A privilege escalation attack is the act of exploiting a security weakness in an application to gain access to resources that normally would have been protected from an application or user. This mcans that low rights users can add files to a directory and overwrite the binaries installed therein, which will be executed by a later user with higher level of rights. The result is that the application performs actions with a higher security context than intended. As an analogy, consider an office worker who has keys to her office and to the front door of thc building, but not to other offices or to the supply closet. By stealing the janitor's master key, the office worker can escalate her privileges. In essence, the MediaMax provides that master key.

The MediaMax software makes such an attack possible by leaving a crucial folder "unlocked." This folder contains an executablc program (MMX.EXE, the MediaMax program), which is necessarily run by a user account with high ("Administrator") privileges. Because the folder is unlocked, an attacker can overwrite MMX.EXE with code of her choice, and the next time a MediaMax disc is played, her attack code will be executed.

Specifically, the directory that the SunnComm MediaMax softwarc crcatcs, located in "c:\Program Files\Common Files\SunnComm Shared\", overrides the default Access Control List (also known as the file system permissions). The SunnComm Shared directory uses an ACL that doesn't protect against low rights users (i.e. "Everyone" in Windows parlance) overwriting the contents including the installed binaries. In addition, one component of MediaMax, a system service called sbcphid, is loaded into memory and ready to run at all times, even when there is no disc in the CD drive and no music is being played. And it runs as a kernel process, meaning that it has access to all aspects of the system.

These flaws in thc SunnComm MediaMax software distributed by Sony BMG could expose the computers of millions of users to attacks by malicious hacker and virus writers. They undermine significant security protections otherwise present on computers running Windows.

We would like to provide Sony BMG with a detailed report about this security flaw and potential exploits in a secure manner. Please advise us on how best to communicate further information about this security concern to the appropriate people on your technical team. Please also advise SunnComm of this security risk as soon as possible or let us know how to best contact them directly.

In addition, we believc it ncccssary to public safety to immediately publicize and address this security risk. Therefore, we plan to take the following steps:

1) We will be advising the public of the existence of a security risk tomorrow, but will delay public disclosure of the details of how the software can be exploited for the time being.

2) We will be providing detailed information to prominent anti-virus and anti-spyware computer security companies to allow them to start addressing the flaw.

3) If necessary, we will also seek a temporary restraining order prohibiting further sales of the MediaMax CDs and mandating an extensive recall notice campaign.

Before we publish a detailed description of the nature of the risk and seek the Court's assistance, we are willing to give Sony BMG a window in which to take significant stcps to rectify the problem, so those steps may be announced along with the publication of further details about the risk and, hopefully, there will be no need for judicial intervention. At a minimum, these steps must include an immediate recall of the MediaMax CDs now in circulation, an extensive publicity campaign to notify consumers of thc rccall and the security problems associated with both the XCP and MediaMax discs, including use of the banner-ad technology that is a feature of both the XCP and MediaMax software.

As you consider your response, we remind you that we have previously identified severe problems with MediaMax discs, including: undisclosed communications with scrvcrs Sony controls whenever a consumer plays a MediaMax CD; undisclosed installation of over 12 MB of software regardless of whether the user agrees to the EULA; and failure to include an uninstaller with the CD. Nevertheless, Sony BMG has refused to take appropriate action to address these concerns. In light of the security problems identified herein, we urge Sony BMG to reconsider its position.

Please let us know by **10 AM Tuesday, December 6**, whether Sony BMG intends to recall the MediaMaxCDs and take necessary measures to notify consumers of the existence of and reasons for the recall. Please also take noticc that if Sony fails to takc these steps, EFF and its co-counsel will have no choice but to apply for a temporary restraining order seeking the aforementioned relief at 8:30 a.m. on Wednesday, December 7, before Judge Victoria Chaney in Los Angeles Superior Court. Please let us know whether Sony will appear to oppose such an application. Plcasc consider this notice of our intent to seek such relief.

This letter is without prejudice to any legal rights our clients may have.

If you have any questions, please contact my colleague Kurt Opsahl or me as soon as possible.

Yours sincerely,

Cindy Cohn
Electronic Frontier Foundation

Robert A Green
Robert Green
Green Welling, LLP

cc: Reed Kathrein, Esq.
Lerach Coughlin Stoia Geller Rudman & Robbins LLP